Fingerprinting Through RPC

Hidenobu Seki

Urity@SecurityFriday.com

Agenda

- Information gathering for RPC troubleshooting
- Microsoft RPC
- Interface IDs of Windows RPC services
- Info gathering without authentication using RPC
- Online password cracking using RPC

Agenda

- Information gathering for RPC troubleshooting
- Microsoft RPC
- Interface IDs of Windows RPC services
- Info gathering without authentication using RPC
- Online password cracking using RPC

Microsoft Portqry

- Reports the status of target TCP/UDP ports on a remote computer.
- Knows how to send a query to the RPC endpoint mapper.

- For more information, refer to KB832919

Portqry for Active Directory

- UUID: ecec0d70-a603-11d0-96b1-00a0c91ece30
  NTDS Backup Interface
  ncacn_np:\\\\MYDC[\\PIPE\\lsass]
- UUID: 16e0cf3a-a604-11d0-96b1-00a0c91ece30
  NTDS Restore Interface
  ncacn_np:\\\\MYDC[\\PIPE\\lsass]
- UUID: e3514235-4b06-11d1-ab04-00c04fc2dcd2
  MS NT Directory DRS Interface
  ncacn_ip_tcp:169.254.0.18[1027]
- UUID: f5cc59b4-4264-101a-8c59-08002b2f8426
  NtFrs Service
  ncacn_ip_tcp:169.254.0.18[1130]

from Microsoft KB310456(=KB816103)

Portqry for Exchange Server

- UUID: f5cc5a18-4264-101a-8c59-08002b2f8426
  MS Exchange Directory NSPI Proxy
  ncacn_http:169.254.112.100[1444]
- UUID: 9e8ee830-4459-11ce-979b-00aa005ffebe
  MS Exchange MTA 'Mta' Interface
  ncacn_np:\\\\mymailsrv[\\pipe\\00000bbc.000]
- UUID: 9e8ee830-4459-11ce-979b-00aa005ffebe
  MS Exchange MTA 'Mta' Interface
  ncacn_ip_tcp:169.254.112.100[2168]
- UUID: 99e64010-b032-11d0-97a4-00c04fd6551d
  Exchange Server STORE ADMIN
  ncadg_ip_udp:169.254.112.100[2174]

from Microsoft KB310298

Annotation

- UUID: e3514235-4b06-11d1-ab04-00c04fc2dcd2
  MS NT Directory DRS Interface
  ncacn_ip_tcp:169.254.0.18[1027]
- UUID: 99e64010-b032-11d0-97a4-00c04fd6551d
  Exchange Server STORE ADMIN
  ncadg_ip_udp:169.254.112.100[2174]

Endpoint

- UUID: ecec0d70-a603-11d0-96b1-00a0c91ece30
  NTDS Backup Interface
  ncacn_np:\\\\MYDC[\\PIPE\\lsass]
- UUID: f5cc5a18-4264-101a-8c59-08002b2f8426
  MS Exchange Directory NSPI Proxy
  ncacn_http:169.254.112.100[1444]

RPC network protocols

- ncacn_ip_tcp
- ncadg_ip_udp
- ncacn_np
- ncalrpc
- ncacn_http

LPC port name or Named Pipe name

- ncalrpc:[SMTPSVC_LPC]
- ncacn_np:\\\\WSRV[\\PIPE\\NNTPSVC]

Interface ID

- UUID: **f5cc59b4-4264-101a-8c59-08002b2f8426**
  NtFrs Service
  ncacn_ip_tcp:169.254.0.18[1130]
- UUID: **9e8ee830-4459-11ce-979b-00aa005ffebe**
  MS Exchange MTA 'Mta' Interface
  ncacn_ip_tcp:169.254.112.100[2168]

Interface ID

- Interface ID is expressed as **U**niversally **U**nique **ID**entifier
- Is useful for fingerprinting
- Interface has version number
- RPC service may have more than one interface ID

Agenda

- Information gathering for RPC troubleshooting
- Microsoft RPC
- Interface IDs of Windows RPC services
- Info gathering without authentication using RPC
- Online password cracking using RPC

Microsoft RPC

- Enables data exchange and invocation of functionality between different processes
  - on the same machine
  - on the local area network
  - across the Internet
- Is an extension to OSF-DCE RPC

RPC defined

- Operation: Procedure
- Interface: Group of Operations
- Service: Provides Interfaces
- Endpoint: Where Service is
- Endpoint map: List of Endpoints
- Endpoint mapper: Supports dynamic binding to Services

RPC traffic over TCP

Client

bind <interface>

bind ack

request <operation>

response

request <operation>

response

Server

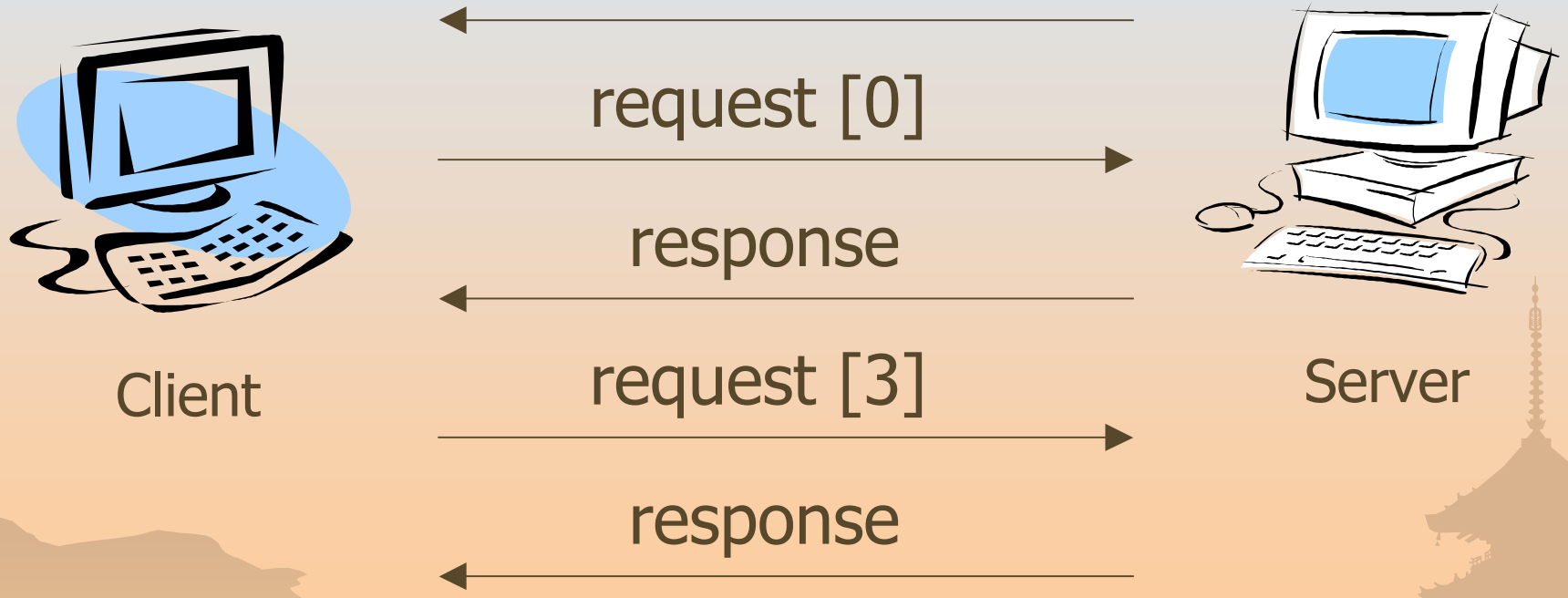
Operations of AT service

- Submit a task
  - JobAdd
- Cancel one or more scheduled tasks
  - JobDel
- View scheduled tasks
  - JobEnum
- Get information of a scheduled task
  - JobGetInfo

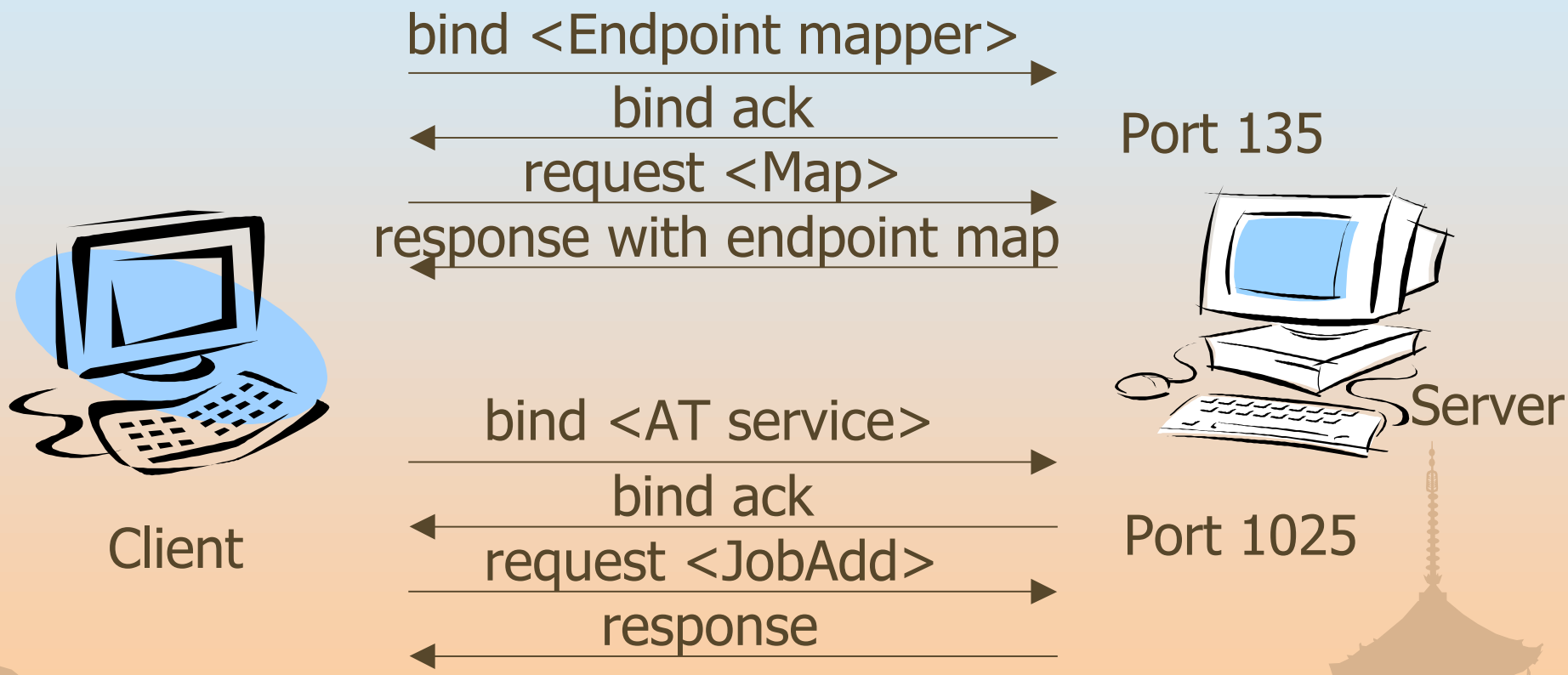
AT service

- Operations: JobAdd,JobDel,JobEnum,JobGetInfo
- Op. No.: 0, 1, 2, 3
- Interface: AT service
- Interface ID: 1ff70682-0a51-30e8-076d-740be8cee98b
- Service: Task Scheduler
- Endpoint: ncacn_ip_tcp:192.168.0.101[1025]

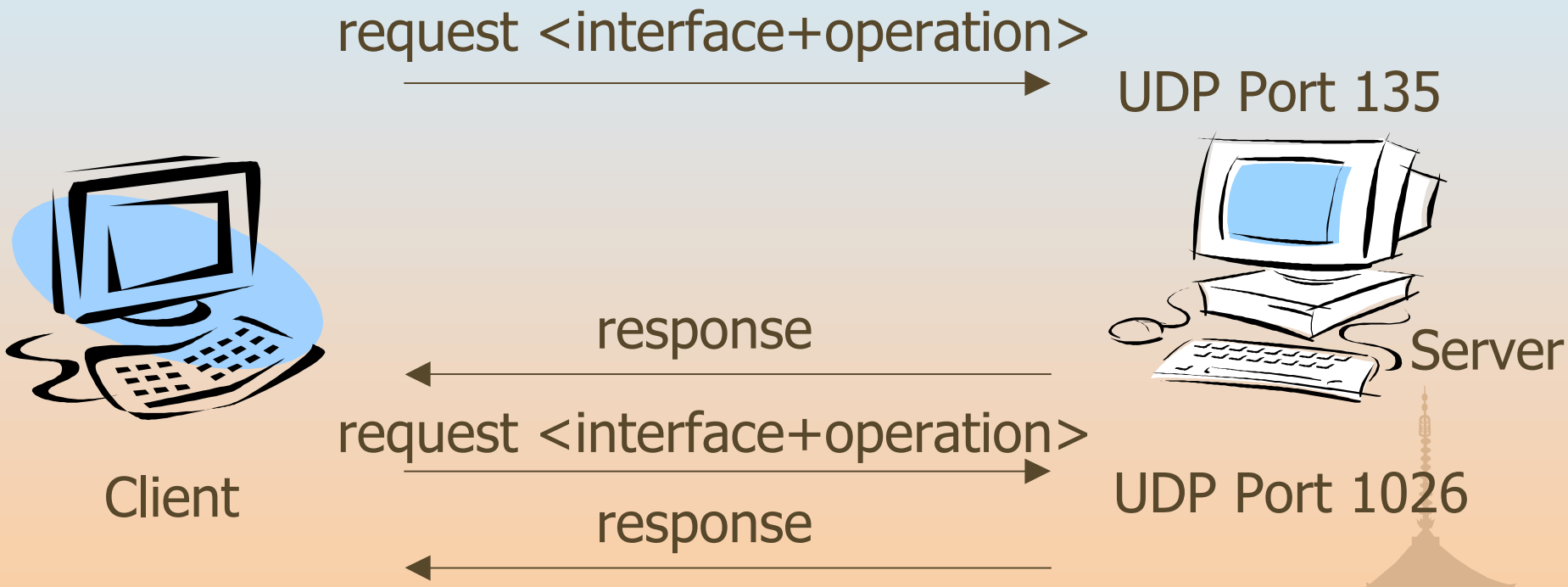
Submit a task, get information



Dynamic binding



Dynamic binding over UDP



Agenda

- Information gathering for RPC troubleshooting
- Microsoft RPC
- Interface IDs of Windows RPC services
- Info gathering without authentication using RPC
- Online password cracking using RPC

Interface IDs of RPCSS

- e1af8308-5d1f-11c9-91a4-08002b14a0fa
- 0b0a6584-9e0f-11cf-a3cf-00805f68cb1b
- e60c73e6-88f9-11cf-9af1-0020af6e72f4
- 99fcfec4-5260-101b-bbcb-00aa0021347a
- b9e79e60-3d52-11ce-aaa1-00006901293f
- 412f241e-c12a-11ce-abff-0020af6e7a17
- 00000136-0000-0000-c000-000000000046
- 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57
- 975201b0-59ca-11d0-a8d5-00a0c90d8051
- c6f3ee72-ce7e-11d1-b71e-00c04fc3111a
- 000001a0-0000-0000-c000-000000000046
- 1d55b526-c137-46c5-ab79-638f2a68e869

Interface IDs of RPCSS

- e1af8308-5d1f-11c9-91a4-08002b14a0fa
  - **Endpoint Mapper**
- 99fcfec4-5260-101b-bbcb-00aa0021347a
  - **IOXIDResolver**
- 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57
  - **IRemoteActivation**
- 00000136-0000-0000-c000-000000000046
  - **ISCMLocalActivator**
- 000001a0-0000-0000-c000-000000000046
  - **ISystemActivator**

Windows NT 4.0

- e1af8308-5d1f-11c9-91a4-08002b14a0fa
- **0b0a6584-9e0f-11cf-a3cf-00805f68cb1b**
  - **Version 1.0**
- e60c73e6-88f9-11cf-9af1-0020af6e72f4
- 99fcfec4-5260-101b-bbcb-00aa0021347a
- b9e79e60-3d52-11ce-aaa1-00006901293f
- 412f241e-c12a-11ce-abff-0020af6e7a17
- 00000136-0000-0000-c000-000000000046
- 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57
- **975201b0-59ca-11d0-a8d5-00a0c90d8051**
  - **NT, 2000**

Windows 2000

- e1af8308-5d1f-11c9-91a4-08002b14a0fa
- **0b0a6584-9e0f-11cf-a3cf-00805f68cb1b**
  - **Version 1.1**
- e60c73e6-88f9-11cf-9af1-0020af6e72f4
- 99fcfec4-5260-101b-bbcb-00aa0021347a
- b9e79e60-3d52-11ce-aaa1-00006901293f
- 412f241e-c12a-11ce-abff-0020af6e7a17
- 00000136-0000-0000-c000-000000000046
- 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57
- **975201b0-59ca-11d0-a8d5-00a0c90d8051**
  - **NT, 2000**
- **c6f3ee72-ce7e-11d1-b71e-00c04fc3111a**
  - **2000, XP, 2003**
- **000001a0-0000-0000-c000-000000000046**
  - **2000, XP, 2003**

Windows XP, 2003

- e1af8308-5d1f-11c9-91a4-08002b14a0fa
- **0b0a6584-9e0f-11cf-a3cf-00805f68cb1b**
  - **Version 1.1**
- e60c73e6-88f9-11cf-9af1-0020af6e72f4
- 99fcfec4-5260-101b-bbcb-00aa0021347a
- b9e79e60-3d52-11ce-aaa1-00006901293f
- 412f241e-c12a-11ce-abff-0020af6e7a17
- 00000136-0000-0000-c000-000000000046
- 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57
- **c6f3ee72-ce7e-11d1-b71e-00c04fc3111a**
  - **2000, XP, 2003**
- **000001a0-0000-0000-c000-000000000046**
  - **2000, XP, 2003**
- **1d55b526-c137-46c5-ab79-638f2a68e869**
  - **XP, 2003**

NT 4.0 Service Pack 4

- DNS server
  - aae9ac90-ce13-11cf-919e-08002be23c64
  - **d7f9e1c0-2247-11d1-ba89-00c04fd91268**
- WINS server
  - 45f52c28-7f9f-101a-b52b-08002b2efabe
  - **811109bf-a4e1-11d1-ab54-00a0c91e9b45**

DNS server

- Windows NT 4.0 SP4 or later
  - aae9ac90-ce13-11cf-919e-08002be23c64
  - d7f9e1c0-2247-11d1-ba89-00c04fd91268
- Windows 2000, 2003
  - 50abc2a4-574d-40b3-9d66-ee4fd5fba076

NT 4.0 with IIS 2.0, 3.0

- World Wide Web Publishing Service
  - 53e75790-d96b-11cd-ba18-08002b2dfead
- FTP Publishing Service
  - 5c89f409-09cc-101a-89f3-02608c4d2361
- Gopher Publishing Service
  - 04fcb220-fcfd-11cd-bec8-00aa0047ae4e

NT 4.0 with IE 5.01

- Task Scheduler
  - 1ff70682-0a51-30e8-076d-740be8cee98b
  - 378e52b0-c0a9-11cf-822d-00aa0051e40f

Task Scheduler

- Windows NT 4.0, 2000
  - 1ff70682-0a51-30e8-076d-740be8cee98b
  - 378e52b0-c0a9-11cf-822d-00aa0051e40f
- Windows XP, 2003
  - 1ff70682-0a51-30e8-076d-740be8cee98b
  - 378e52b0-c0a9-11cf-822d-00aa0051e40f
  - **0a74ef1c-41a4-4e06-83ae-dc74fb1cdd53**

SMTP service of IIS

- IIS 4.0 (NT)
  - 8cfb5d70-31a4-11cf-a7d8-00805f48a135
- IIS 5.0 or later (2000, XP, 2003)
  - 8cfb5d70-31a4-11cf-a7d8-00805f48a135
  - **906b0ce0-c70b-1067-b317-00dd010662da**

DHCP server

- Windows NT 4.0
  - 6bffd098-a112-3610-9833-46c3f874532d
- Windows 2000, 2003
  - 6bffd098-a112-3610-9833-46c3f874532d
  - **5b821720-f63b-11d0-aad2-00c04fc324db**

Message Queuing service

- 2000, XP, 2003
  - fdb3a030-065f-11d1-bb9b-00a024ea5525
  - 76d12b80-3467-11d3-91ff-0090272f9ea3
  - 1088a980-eae5-11d0-8d9b-00a02453c337
  - 41208ee0-e970-11d1-9b9e-00e02c064c39
- 2000
  - 5b5b3580-b0e0-11d1-b92d-0060081e87f0
- XP
  - 5b5b3580-b0e0-11d1-b92d-0060081e87f0
  - 7e048d38-ac08-4ff1-8e6b-f35dbab88d4a
  - fc13257d-5567-4dea-898d-c6f9c48415a0
- 2003
  - fc13257d-5567-4dea-898d-c6f9c48415a0
  - 1a9134dd-7b39-45ba-ad88-44d01ca47f28

SQL Server 7.0, 2000

- Interface ID
  - 3f99b900-4d87-101b-99b7-aa0004007f07
- SQL Server 2000
  - Multiprotocol Net-Library using RPC is not installed by default

Messenger Service

- Used to have two IDs

1. 5a7b91f8-ff00-11d0-a9b2-00c04fb6e6fc
   - Removed by MS03-043 patch
   - ncalrpc:[DNSResolver]
     - » Windows 2000 Service Pack 3, 4 installed
2. 17fdd703-1827-4e34-79d4-24a55c53bb37

XP Service Pack 1

- SSDP Discovery service
  - 4b112204-0e19-11d3-b42b-0000f81feb9f
  - svchost.exe -k LocalService
  - After local logon

- "System Services for the Windows Server 2003 Family and Windows XP Operating Systems" on Microsoft TechNet

XP with SP1: Home or Professional

- Remote Registry Service
  - Installed in XP Professional only
  - ncacn_np:\\\\FOO[\\PIPE\\winreg]

Identifying Interface IDs of RPC services

- Start/Stop Service
- Fport or netstat -ano
  - Match TCP/UDP port of endpoint to process
- Search ID in Registry
  - HKEY_CLASSES_ROOT\Interface
- Search ID in binary files
- Google

UUID in EXE/DLL files

- 5a7b91f8-ff00-11d0-a9b2-00c04fb6e6fc
- f8917b5a 00ff d011 a9b2 00c04fb6e6fc
  - unsigned long
  - unsigned short
  - unsigned short
  - unsigned char [2]
  - unsigned char [6]

Interface IDs and Operations of RPC services over SMB

- Samba IDL files
  http://www.samba.org/cgi-bin/cvsweb/samba4/source/librpc/idl/

More Interface IDs, Operations, etc.

- "Windows network services internals"
  by Jean-Baptiste Marchand

  http://www.hsc.fr/
  ressources/articles/win_net_srv/index.html.en

Agenda

- Information gathering for RPC troubleshooting
- Microsoft RPC
- Interface IDs of Windows RPC services
- Info gathering without authentication using RPC
- Online password cracking using RPC

XP, 2003: svchost.exe –k netsvcs

6to4, AppMgmt, AudioSrv, Browser, CryptSvc, DMServer, DHCP, ERSvc, EventSystem, FastUserSwitchingCompatibility, HidServ, Ias, Iprip, Irmon, **LanmanServer**, **LanmanWorkstation**, Messenger, Netman, Nla, Ntmssvc, NWCWorkstation, Nwsapagent, Rasauto, Rasman, Remoteaccess, **Schedule**, Seclogon, SENS, Sharedaccess, SRService, Tapisrv, Themes, TrkWks, W32Time, WZCSVC, Wmi, WmdmPmSp, winmgmt, TermService, wuauserv, BITS, ShellHWDetection, helpsvc, Uploadmgr, WmdmPmSN

Exposed interfaces

Binding	Object UUID / Interface identifier	Annotation	Remark by Urity	Remark2 by Urity
ncacn_ip_tcp:192.168.0.5[1025]			Task Scheduler	Internet Explorer 5.01 or later
	ce1334a5-41dd-40ea-881d-64326b23effe		Infrared Monitor	
	209bb240-b919-11d1-bbb6-0080c75e4ec1		Infrared Monitor	
	5ca4a760-ebb1-11cf-8611-00a0245420ed		Terminal Services	
	621dff68-3c39-4c6c-aae3-e68e2c6503ad		Wireless Zero Configuration	
	00000134-0000-0000-c000-000000000046			IRundown
	18f70770-8e64-11cf-9af1-0020af6e72f4			
	00000131-0000-0000-c000-000000000046			IRemUnknown
	00000143-0000-0000-c000-000000000046			IRemUnknown2
	00000132-0000-0000-c000-000000000046			IObjServer
	1ff70682-0a51-30e8-076d-740be8cee98b		Task Scheduler	Internet Explorer 5.01 or later
	378e52b0-c0a9-11cf-822d-00aa0051e40f		Task Scheduler	Internet Explorer 5.01 or later
	0a74ef1c-41a4-4e06-83ae-dc74fb1cdd53		Task Scheduler	Windows XP or Windows Server 2003
	3faf4738-3a21-4307-b46c-fdda9bb8c0d5		Windows Audio	Windows XP or Windows Server 2003
	6bffd098-a112-3610-9833-46c3f87e345a		Workstation service	
	8d0ffe72-d252-11d0-bf8f-00c04fd9126b		Protected Storage or Cryptographic Services	
	a3b749b1-e3d0-4967-a521-124055d1c37d		Cryptographic Services	Windows XP or Windows Server 2003
	0d72a7d4-6148-11d1-b4aa-00c04fb66ea0		Protected Storage or Cryptographic Services	
	f50aac00-c7f3-428e-a022-a6b71bfb9d43		Cryptographic Services	Windows XP or Windows Server 2003
	12b81e99-f207-4a4c-85d3-77b42f76fd14		Secondary Logon	Windows XP or Windows Server 2003
	4b324fc8-1670-01d3-1278-5a47bf6ee188		Server Service	
	300f3532-38cc-11d0-a3f0-0020af6b0add		Distributed Link Tracking Client	
	3f77b086-3a17-11d3-9166-00c04f688e28		System Restore Service	Windows XP or Windows Server 2003
	17fdd703-1827-4e34-79d4-24a55c53bb37		Messenger Service	
	64b8f404-a4ae-11d1-b7b6-00c04fb926af			IEventSystemTier2Factory
	63fbe424-2029-11d1-8db8-00aa004abd5e		System Event Notification	
	629b9f66-556c-11d1-8dd2-00aa004abd5e		System Event Notification	
	8fb6d884-2388-11d0-8c35-00c04fda2795		Windows Time	
	00000001-0000-0000-c000-000000000046			IClassFactory
	6bffd098-a112-3610-9833-012892020162		Computer Browser	

XP, 2003: Using exposed interface of Server service

- RemoteTOD
  - Get time and date information
  - Without authentication
- ServerGetInfo
  - Get server name, type and OS version
    - » Domain Controller, SQL Server, Terminal Server
  - With null user and null password authentication
- ShareEnum
  - Get information about all shared resource
  - With null user and null password authentication

XP: Using exposed interface

- SessionEnum (Server service)
  - Get information about all users logged on remotely
  - With null user and null password authentication
- WkstaUserEnum (Workstation service)
  - Get information about all users logged on locally
  - Without authentication

Using exposed interface

- Demo

Gathering RPC information without endpoint map

- Do a port scan
- Send “is_server_listening”
  - Ask whether a server is listening for RPC
- Send “inq_if_ids”
  - Inquire all interface IDs of the service

Remote Management Interface

- Is implemented by all RPC services in an interoperable manner
- No need for authentication using RMI operations
- afa8bd80-7d8a-11c9-bef4-08002b102989

- Operation No.0 = inq_if_ids
- Operation No.2 = is_server_listening

XP Service Pack 2

- RPC interface restriction through user authentication
- Strong possibility of RMI being restricted

Agenda

- Information gathering for RPC troubleshooting
- Microsoft RPC
- Interface IDs of Windows RPC services
- Info gathering without authentication using RPC
- Online password cracking using RPC

Online password cracking

- Need the following information
  - Interface IDs
  - Operations and arguments
  - Results, such as type of errors

Even if the information is unavailable

- Use Remote Management Interface
  - With authentication **!**
  - Send “is_server_listening”
  - Error status of access denied is 0x05

Online password cracking

- Demo

When the password is cracked

- Schedule commands through AT service
- Demo
  - ncacn_ip_tcp:192.168.0.101[1025]

Well-known endpoint dump tools with source code

- rpcdump by Sir Dystic [cDc]
- rpctools by Todd Sabin
- dcedump in SPIKE by Dave Aitel

RpcScan by Urity

- Released June 2003
- No new dump techniques
- Over 10,000 downloads last year

Summary

- Interface IDs of Windows RPC services
- Info gathering without authentication using RPC
- Online password cracking using RPC

Special thanks to Sir Dystic [cDc]